



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,873	11/22/2005	Marc Joye	032326-301	6724
21839	7590	02/17/2011		
BUCHANAN, INGERSOLL & ROONEY PC POST OFFICE BOX 1404 ALEXANDRIA, VA 22313-1404				EXAMINER
				WRIGHT, BRYAN F
ART UNIT		PAPER NUMBER		
		2431		
NOTIFICATION DATE		DELIVERY MODE		
02/17/2011		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com
offserv@bipc.com

Office Action Summary	Application No. 10/534,873	Applicant(s) JOYE ET AL.
	Examiner BRYAN WRIGHT	Art Unit 2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 16 August 2010.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-13 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-13 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date _____
 5) Notice of Informal Patent Application
 6) Other: _____

DETAILED ACTION

In view of the Appeal Brief filed on 8/16/2010, PROSECUTION IS HEREBY REOPENED. A new ground of rejection cited under Applicant's Admitted Prior Art, the well known "Pencil/Paper Method" and prior art reference Miyaguichi. To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid. A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below. Claims 1, 2, 4, 5, 7, 8 9, 12 and 13 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2431

2. Claims 1, 2, 4, 5, 7, 8 9, 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admitted Prior Art (hereinafter "Pencil/Paper Method" (Page 2, lines 25-40, Page 3, lines 10-31 & Page 4, lines 1-25)) in view of Miyaguichi (US Patent No. 4,514,592).

3. As to claim 1, Pencil/Paper Method teaches a cryptographic method during which an integer division of the type $q = a \text{ div } b$ and $r = a \text{ mod } b$ (i.e., ...teaches integer division to obtain q and r [page 3, lines 15-30] with where q is a quotient [page 3, lines 15-30], a is a number of containing m bits [page 3, lines 15-30], b is a number of containing n bits [page 3, lines 15-30], with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of b [page 3, lines 15-30], comprising the following steps: (i) performing a partial division of a word A [page 3, lines 15-30], comprising n bits of the number a, by the number b to obtain a bit of the quotient q, (i.e., ...teaches integer division [page 3, lines 15-30];

(iii) generating encrypted or decrypted data in accordance with said quotient (i.e., ...teaches cryptographic (e.g., encrypt/decrypt) methods using integer division (e.g., quotient) [page 2, lines 25-40] ...On page 3, lines 15-30 states a well known method (e.g., cryptographic method) is the "Pencil Paper Method"),

(ii) repeating step (i) for $m-n + 1$ iterations (e.g., For Loop) with the same number and type operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q. (i.e.... the well known "Pencil/Paper Method" disclosed in Applicant's Admitted Prior Art discloses instructions for which are

implemented as a "Computer For Loop Condition Statement" for iterative calculation of the encryption process as recited in Applicant's Specification; pages 3-5.

Pencil/Paper does not expressly teach integer division performed in a processor of an electronic device. However, the Examiner contends that Miyaguichi disclosed at the time of applicant's original filings an electronic component (e.g., device) for integer division. See Miyaguichi column 13, lines 18-30. Therefore given the Pencil/Paper division method, a person of ordinary skill in the art would have recognized the advantage of modifying the method to enhance processing time and capability with Miyaguichi's capability to perform integer division calculations electronically.

4. As to claim 2, Pencil/Paper Method discloses a method where at each iteration, an addition of the number b to the word A and a subtraction of the number b from the word A are performed (i.e., ...the Examiner notes that the Pencil/Paper method discloses both subtract (SUB) and addition (ADD) operations. With regards to applicant's claim limitation element of "each iteration", the Examiner notes that despite the ADD operation being part of a conditional IF/THEN statement, there exists a state of the FOR Loop where the ADD operation will be performed the same number of times (e.g., iteration) as the SUB operation. Such a state would mean that the both ADD and SUB operations are performed for each loop iteration. [col. 4, lines 15-22]).

5. As to claim 3, (Cancelled).

6. As to claim 4, Pencil/Paper Method discloses where, at each iteration, either the number b or the number b complementary to the number b is added to the word A. (i.e., ...teaches on page 8, lines 1-15 that at each iteration a (b) value and complementary (b) value is part of an addition process).

7. As to claim 5, Pencil/Paper Method discloses a method further including the step, at each iteration, of updating a first variable (c') indicating whether (i.e., ...teaches updating variable (o') after each iteration [page 7, lines 5-10]), during the following iteration, the number b or the complementary to the number b is to be added with the word A according to the quotient bit produced (i.e., ...teaches on page 8, lines 1-15 that at each iteration a (b) value and complementary (b) value is part of an addition process).

8. 6. (Canceled)

9. As to claim 7, Pencil/Paper Method discloses a method 'further including the steps, at each iteration, of performing an operation of complement to 2^n of an updated data item (b or b complement) or of a notional data item (c or c complement) (i.e.,...teaches using the complement [page 8, lines 5-10]), and adding the updated data item with the word A.

10. As to claim 8, Pencil/Paper Method discloses a method further including the step, at each iteration, of updating a second variable (i.e., ...teaches updating variable (o) after each iteration [page 7, lines 10-15]), indicating whether, during the following iteration, the operation of complement to $2n$ is to be performed on the updated data item or on the notional data item (i.e.,...teaches using the complement [page 8, lines 5-10]).

11. As to claims 12 and 13, Pencil/Paper Method discloses a cryptographic method using an integer division, however the Pencil/Paper method does not disclose an electronic component comprising calculation means programmed to implement a method, said calculation means comprising a central unit associated with a memory comprising several registers for storing the data a and b and a chip card comprising an electronic component according to Claim 12. However the Examiner contends that Miyaguichi disclosed an electronic component (e.g., device) for integer division. See Miyaguichi column 13, lines 18-30. Therefore given the Pencil/Paper division method, a person of ordinary skill in the art would have recognized the advantage of modifying the method to enhance processing time and capability with Miyaguichi's capability to perform integer division calculations electronically.

Allowable Subject Matter

Claim 9 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431